REMARKS

I. INTRODUCTION

In response to the Office Action dated December 31, 2003, no claims have been canceled, amended or added. Claims 1-3, 5-42, 44-81 and 83-117 remain in the application. Entry of these remarks, and re-consideration of the application is requested.

II. PRIOR ART REJECTIONS

A. The Office Action Rejections

In paragraphs (2)-(3) of the Office Action, claims 1, 5-11, 14, 16, 17, 21, 22, 40-50, 53, 55, 56, 60, 61, 79, 83-89, 92, 94, 95, and 100 were rejected under 35 U.S.C. §103(a) as being unpatentable over Freier et al. (Freier) in view of Weinstein et al., U.S. Patent No. 6,094,485 (Weinstein). In paragraph (4) of the Office Action, claims 2, 28-39, 41, 67-78, 80, and 106-117 were rejected under 35 U.S.C. §103(a) as being unpatentable over Freier in view of Weinstein and further in view of Fryer et al. "Microsoft Press Computer Dictionary," 1997, Microsoft Press, 3rd Edition, pg. 320 (Fryer). In paragraph (5) of the Office Action, claims 12, 51, and 90 were rejected under 35 U.S.C. §103(a) as being unpatentable over Freier in view of Weinstein and further in view of Griffiths et al. (Griffiths). In paragraph (6) of the Office Action, claims 13, 52, and 91 were rejected under 35 U.S.C. §103(a) as being unpatentable over Freier in view of Weinstein and further in view of the Netscape Handbook (Netscape). In paragraph (7) of the Office Action, claims 15, 18-20, 23-25, 54, 57-59, 62-64, 93, 96-98, and 101-103 were rejected under 35 U.S.C. §103(a) as being unpatentable over Freier in view of Weinstein and further in view of Coley et al. (Coley). In paragraph (8) of the Office Action, claims 26, 65, and 104 were rejected under 35 U.S.C. §103(a) as being unpatentable over Freier in view of Weinstein and further in view of Raz. In paragraph (9) of the Office Action, claims 27, 66, and 105 were rejected under 35 U.S.C. §103(a) as being unpatentable over Freier in view of Weinstein and Raz, and further in view of Coley.

Applicants' attorney respectfully traverses these rejections.

B. The Applicants' Claimed Invention

Independent claims 1, 40 and 79 are generally directed to a network multiplexing and tunneling system, transmission media and method. The method of claim 79 is representative and comprises:

(a) opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network;

(b) establishing a secure connection using Secure Sockets Layer (SSL) over the opened Transmission Control Protocol (TCP) connection;

(c) mutually authenticating each of the endpoints of the secure connection; and

(d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated, wherein either endpoint of the secure connection can receive connection requests for the multiplexed other connections.

C. The Freier Reference

Freier describes Version 3.0 of the Secure Sockets Layer (SSL V3.0) protocol, a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

D. The Weinstein Reference

Weinstein describes a process that allows an exportable SSL client to negotiate an encrypted session using strong encryption with a server if the server is allowed to use strong encryption. With this process, the SSL client is normally limited to export strength encryption. But, when it is communicating with an approved server, it is able to expand the available set of encryption algorithms to include stronger algorithms/key lengths. The process involves performing an SSL handshake twice. The process begins when a client, i.e. a user, wants to establish a session with a server. The client first initiates a network connection to the server. The first handshake between an export client and an approved server results in an SSL session that uses export strength encryption. This establishes a connection using an exportable cipher suite. The client examines the server's certificate obtained as part of the first handshake. If the server is not approved, the SSL session transfers application data that are protected by the export cipher. If the server is approved, then the client initiates a second handshake, this time allowing stronger cipher suites. The result of the second handshake is an SSL session that uses strong encryption. The SSL session may then be used to transfer application data that are protected by the strong cipher suite. At this point, the process is complete.

E. The Fryer Reference

Fryer describes is a dictionary of computer terms, wherein the cited pages provide a definition of UDP (User Datagram Protocol).

F. The Griffiths Reference

Griffiths describes a system for storing information on a computer network and allowing the information to be accessed by terminals connected to the computer network, either directly, or through an intermediary device such as a local or proxy server, includes computer or web sites which store pages requested by terminals for display on the terminals. The pages may include references to banners to be displayed in conjunction with the web pages on the terminal. The terminal initiates access or connection to a desired computer or web site to access a desired page. After the desired page is downloaded, transmitted, or served to the terminal from the computer or web site, the terminal initiates and sends an initial banner request signal to an information server. The information server returns a redirect signal to the terminal telling the terminal the location of the desired banner on the computer network, which may be the information server, the computer site, or some other information server, computer site, or location accessible via the computer network. The terminal then initiates a second banner request signal to the location of the desired banner and the banner is served to the terminal for display on the terminal, unless the requested banner has previously been stored or cached in the terminal's memory or in the memory of a local or proxy server connected to the terminal, in which case the second banner request signal is not sent across the computer network and the banner is loaded directly from the terminal's memory or served to the terminal from the proxy server.

G. The Netscape Reference

Netscape is a handbook that describes the SOCKS protocol.

H. The Coley Reference

Coley describes providing a firewall for isolating network elements from a publicly accessible network to which such network elements are attached. The firewall operates on a stand alone computer connected between the public network and the network elements to be protected such that all access to the protected network elements must go through the firewall. The firewall application running on the stand alone computer is preferably the only application running on that

machine. The application includes a variety of proxy agents that are specifically assigned to an incoming request in accordance with the service protocol (i.e., port number) indicated in the incoming access request. An assigned proxy agent verifies the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request.

I. The Raz Reference

Raz describes an information transfer network, comprising: a plurality of client terminals which comprise a presentation system having a control and management agent system; a plurality of servers which comprise a database system and an application system, and a control and management agent system; a request broker system which permits the exchange of information between said client terminals and said servers through a communication path between said terminal and said server, and an information management system for dynamically controlling the location, access and transfer of information between said client terminals and said servers through a plurality of communication paths connecting said control and management agent system of each of said client terminals and servers to said information management system.

J. The Applicants' Claims Are Patentable Over The References

Applicants' invention, as recited in independent claims 1, 40 and 79, is patentable over the references, because the claims recite a specific combination of limitations not found in the references. Specifically, the references do not teach or suggest the specific sequence of steps comprising: (a) opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network; (b) establishing a secure connection using Secure Sockets Layer (SSL) over the opened Transmission Control Protocol (TCP) connection; (c) mutually authenticating each of the endpoints of the secure connection; and (d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated, wherein either endpoint of the secure connection can receive connection requests for the multiplexed other connections.

Nonetheless, the Office Action states the following:

> As per claims 1, 5, 40, 44, 79, and 83, it is disclosed by Freier et al of establishing an SSL session that includes multiple secure (network) connections and parties may have multiple simultaneous (multiplexed) sessions (tunnels)(pg 9-10,

Section 5.1). The SSL protocol is configured to establish a (single) secure (encrypted) connection (tunnel) between a client and a server communicating across an insecure channel whereby both parties (client and server) are authenticated to each other (after the secure connection is opened)(pg 49, Section F & F.1.1). At a lowest level, SSL is layered on top of TCP (user level) which is a transport protocol (pg 3, Section 1). The teachings of Freier et al recite of establishing an SSL session that includes multiple secure (network) connections and parties may have multiple simultaneous (multiplexed) sessions (tunnels)(pg 9-10, Section 5.1) whereby it is interpreted by the examiner that either endpoints can receive connection requests for the simultaneous (multiplexed) connections. The teachings are silent in disclosing of either of the endpoints of the being able to receive data or receive connection requests. The teachings of Weinstein et al disclose of either client and server (endpoints) being able to receive data or connection requests (col. 2, lines 23-34 and col. 8, lines 38-44 & 53-61). It would have been obvious to a person of ordinary skill in the art to have been motivated to apply a means of being able to receive data and to receive connection requests. It is notoriously well known to one of skill that in order to establish a connection between two parties (endpoints), one of the parties (endpoints) have to initiate the connection whereby the other receives the request for connection and if the connection is authenticated, the connection is permitted between the two as is taught by Weinstein et al (col. 2, lines 23-34). Additionally, the teachings of Freier et al disclose of establishing a secure tunnel between two parties (endpoints) whereby it is notoriously well known that either of the two can receive data wherein one of the locations is a sender and the other is the recipient of the information. It is obvious that the teachings of Freier et al comprise the features of at least one of the parties (endpoints) being able to receive connection requests and to receive data for that is the intent of the teachings to establish a secure tunnel (connection) which mutually authenticates both parties (endpoints) and upon successful authentication, secure communications is permitted which would include the sending and receiving of data (pg 49, Section F & F.1.1) and which is additionally disclosed by the teachings of Weinstein et al for support to the teachings of Freier et al (col. 2, lines 23-34 and col. 8, lines 38-44 & 53-61).

Applicants' attorney disagrees. Specifically, Applicants' attorney asserts that Freier and Weinstein do not teach or suggest the combination of limitations found in Applicants' independent claims. For example, at the indicated locations, Freier and Weinstein merely set forth the following:

> Freier: pages 9-10, Section 5.1
> 5.1 Session and connection states
>
> An SSL session is stateful. It is the responsibility of the SSL Handshake protocol to coordinate the states of the client and server, thereby allowing the protocol state machines of each to operate consistently, despite the fact that the state is not exactly parallel. Logically the state is represented twice, once as the current operating state, and (during the handshake protocol) again as the pending state. Additionally, separate read and write

states are maintained. When the client or server receives a change cipher spec message, it copies the pending read state into the current read state. When the client or server sends a change cipher spec message, it copies the pending write state into the current write state. When the handshake negotiation is complete, the client and server exchange change cipher spec messages (see Section 5.3), and they then communicate using the newly agreed-upon cipher spec.

An SSL session may include multiple secure connections; in addition, parties may have multiple simultaneous sessions.

The session state includes the following elements:

session identifier
: An arbitrary byte sequence chosen by the server to identify an active or resumable session state.

peer certificate
: X509.v3[X509] certificate of the peer. This element of the state may be null.

compression method
: The algorithm used to compress data prior to encryption.

cipher spec
: Specifies the bulk data encryption algorithm (such as null, DES, etc.) and a MAC algorithm (such as MD5 or SHA). It also defines cryptographic attributes such as the hash_size. (See Appendix A.7 for formal definition)

master secret
: 48-byte secret shared between the client and server.

is resumable
: A flag indicating whether the session can be used to initiate new connections.

The connection state includes the following elements:

server and client random
: Byte sequences that are chosen by the server and client for each connection.

server write MAC secret
: The secret used in MAC operations on data written by the server

client write MAC secret
: The secret used in MAC operations on data written by the client.

server write key
: The bulk cipher key for data encrypted by the server and decrypted by the client.

client write key
: The bulk cipher key for data encrypted by the client and decrypted by the server.

initialization vectors
: When a block cipher in CBC mode is used, an initialization vector (IV) is maintained for each key. This field is first initialized by the SSL handshake protocol. Thereafter the final ciphertext block from each record is preserved for use with the following record.

sequence numbers
: Each party maintains separate sequence numbers for transmitted and received messages for each connection. When a party sends or receives a change cipher spec message, the appropriate sequence number is set to zero. Sequence

Freier: page 49, Sections F and F.1.1

F.1 Handshake protocol

The handshake protocol is responsible for selecting a CipherSpec and generating a MasterSecret, which together comprise the primary cryptographic parameters associated with a secure session. The handshake protocol can also optionally authenticate parties who have certificates signed by a trusted certificate authority.

F.1.1 Authentication and key exchange

SSL supports three authentication modes: authentication of both parties, server authentication with an unauthenticated client, and total anonymity. Whenever the server is authenticated, the channel should be secure against man-in- the-middle attacks, but completely anonymous sessions are inherently vulnerable to such attacks. Anonymous servers cannot authenticate clients, since the client signature in the certificate verify message may require a server certificate to bind the signature to a particular server. If the server is authenticated, its certificate message must provide a valid certificate chain leading to an acceptable certificate authority. Similarly, authenticated clients must supply an acceptable certificate to the server. Each party is responsible for verifying that the other's certificate is valid and has not expired or been revoked.

The general goal of the key exchange process is to create a pre_master_secret known to the communicating parties and not to

attackers. The pre_master_secret will be used to generate the master_secret (see Section 6.1). The master_secret is required to generate the finished messages, encryption keys, and MAC secrets (see Sections 5.6.9 and 6.2.2). By sending a correct finished message, parties thus prove that they know the correct pre_master_secret.

Freier: page 3, Section 1
1. Introduction

The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP[TCP]), is the SSL Record Protocol. The SSL Record Protocol is used for encapsulation of various higher level protocols. One such encapsulated protocol, the SSL Handshake Protocol, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data. One advantage of SSL is that it is application protocol independent. A higher level protocol can layer on top of the SSL Protocol transparently. The SSL protocol provides connection security that has three basic properties:

- The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES[DES], RC4[RC4], etc.)
- The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA[RSA], DSS[DSS], etc.).
- The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations.

Weinstein: col. 8, lines 38-44
SSL is a layered protocol. At each layer, messages may include fields for length, description, and content. SSL takes messages to be transmitted, fragments the data into manageable blocks, optionally compresses the data, applies a MAC, encrypts, and transmits the result. Received data are decrypted, verified, decompressed, and reassembled, then delivered to higher level clients.

Weinstein: col. 8, lines 53-61 (actually lines 46-61)
An SSL session is stateful. It is the responsibility of the SSL handshake protocol to coordinate the states of the client and server, thereby allowing the protocol state machines of each to operate consistently, despite the fact that the state is not exactly parallel. Logically the state is represented twice, once as the current operating state, and (during the handshake protocol) again as the pending state.

> Additionally, separate read and write states are maintained. When the client or server receives a change cipher spec message, it copies the pending read state into the current read state. When the client or server sends a change cipher spec message, it copies the pending write state into the current write state. When the handshake negotiation is complete, the client and server exchange change cipher spec messages, and then communicate using the newly agreed upon cipher spec.

Applicants' attorney respectfully asserts that the combination of the above references does not teach or suggest (a) opening a single Transmission Control Protocol (TCP) connection at a user-level between at least two endpoints in the network, (b) establishing a secure connection using Secure Sockets Layer (SSL) over the opened Transmission Control Protocol (TCP) connection, (c) mutually authenticating each of the endpoints of the secure connection, and (d) multiplexing other connections through the secure connection once both of the endpoints have been authenticated, wherein either endpoint of the secure connection can receive connection requests for the multiplexed other connections.

Freier and Weinstein, even when combined, do not teach or suggest this specific sequence of steps. Instead, Freier merely describes SSL sessions, states that an SSL session may include multiple secure connections and multiple simultaneous sessions, describes SSL's authentication modes, and states that the SSL Record Protocol as being layered on top of a transport protocol such as TCP. Similarly, Weinstein merely describes SSL as a layered protocol and an SSL session as stateful.

As a result, Applicants' attorney asserts that the combination of references does not teach or suggest that either of the endpoints of a secure connection can receive connection requests, in the context of a single Transmission Control Protocol (TCP) connection at a user-level between the endpoints, where a secure connection using Secure Sockets Layer (SSL) has been established over the opened TCP connection, where each of the endpoints have been mutually authenticated, and where other connections are multiplexed through the secure connection once both of the endpoints have been authenticated.

The remaining references fail to overcome the deficiencies of Freier and Weinstein. For example, Fryer was cited merely for describing UDP as a connectionless protocol within TCP/IP; Griffiths was cited merely for resolving domain names; Netscape was cited merely for describing the use of SOCKS as a means for accessing information on the Internet; Coley was cited merely for using a bastion firewall host computer; and Raz was cited merely for using multiple Intranets.

Moreover, the various elements of Applicants' claimed invention together provide operational advantages over the cited references. In addition, Applicants' invention solves problems not recognized by the cited references.

Thus, Applicants submit that independent claims 1, 40 and 79 are allowable over the cited references. Further, dependent claims 2-3, 5-39, 41-42, 44-78, 80-81 and 83-117 are submitted to be allowable over the cited references in the same manner, because they are dependent on independent claims 1, 40 and 79, respectively, and thus contain all the limitations of the independent claims. In addition, dependent claims 2-3, 5-39, 41-42, 44-78, 80-81 and 83-117 recite additional novel elements not shown by the cited references.

III. CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited.

Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicants

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: February 26, 2004

By: _____
Name: George H. Gates
Reg. No.: 33,500

GHG/